

### Remarks

Claims 1-5 are pending in this application. Claims 1-5 stand rejected by BrachtI et al. (U.S. Patent No. 4,747,050; hereafter "BrachtI"). Claim 1 is amended herewith. The prior art rejections are addressed below.

### Rejections under 35 U.S.C. 102

Claims 1-5 were rejected under 35 USC 102(e) as being anticipated by BrachtI. These rejections are respectfully traversed.

To anticipate a claim, the reference must teach every element of the claim: "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). See MPEP 2131. This standard has not been met in the present case for the following reasons.

**With respect to claim 1, the consumer of BrachtI requires an identity card for authentication whereas the User of the present invention does not.**

According to col. 5 lines 14-17 of BrachtI: "each user of the EFT system has a personal secure intelligent bank card on which is stored a personal account number (PAN) and a personal key (KP)." See also col. 3 lines 48-51. BrachtI further explains in col. 10 lines 3-6 that "[a] transaction is initiated at a POS terminal when a customer's user card is inserted in the EFT module" and that, "[i]nsertion of the card couples the power and data bus connections to the personal portable microprocessor." Thus, BrachtI substantially differs from the present invention in that the user of BrachtI requires an identity card to receive a PAN/KP and for authentication. In other words, it is impossible for the user of BrachtI to be authenticated *without* a personal identity card (wherein the PAN and PK are stored on the card and are only communicated upon the card electrically interfacing with the EFT module).

Claim 1 as amended specifies that the User does not require a personal identity card to receive or use digital identity. As is clear throughout the specification, the only elements required for positive identification or authentication are the three disclosed "entities" in communication with one another and digital identity. As a result of the disclosed digital identity, the present invention provides a system that is simple for businesses to adopt (e.g., wherein they don't need to invest in expensive EFT terminals such as those disclosed by BrachtI). A further advantage of digital identity is that the User doesn't need to worry about lost or stolen identification cards or remembering a separate PIN.

For the above described reasons, Applicants' submit that claim 1 and its dependent claims 2-4 are allowable over the prior art.

**Regarding claim 3, Brachtl does not teach a digital identity comprising a dynamic, non-predictable and time dependent SecureCode provided by the Central-Entity to the User.**

Brachtl does not teach a Central-Entity that provides a dynamic, non-predictable and time dependent SecureCode (as part of digital identity) to the User. Rather, Brachtl discloses that generation of a time-variant parameter takes place either *on the user card or at the EFT terminal* (see col. 5 lines 29-31). Applicants' also point out that neither the personal account number (PAN) nor the personal key (KP) stored on the card (as provided by the card issuing agency) are dynamic, non-predictable and time-dependent.

Another fundamental difference with respect to Brachtl is that determination of a valid PIN takes place at the EFT terminal (abstract, col. 5 lines 3-8). Conversely, the SecureCode of the present invention allows User verification to take place at the Central-Entity – hence avoiding any need for EFT terminals or personal identity cards.

For the above described reasons, Applicants' submit that claim 3 is also allowable over the prior art on its own merit.

**With respect to claim 5, Brachtl does not teach all of the method steps as claimed.**

Brachtl does not teach wherein a "Central-Entity generates a dynamic, non-predictable and time dependent SecureCode" and "sends out the SecureCode to the user over a communication network." Rather, Brachtl discloses that generation of the time-variant parameter starts out either *on the user card or at the EFT terminal* (see col. 5 lines 29-31).

In paper number 091905, it was suggested in paragraph 5 that "the user requests SecureCode from the Central-Entity" corresponds to "where the user receives his unique PAN and PIN." Applicants' respectfully disagree and submit that neither of the PAN, KP, or PIN are dynamic, non-predictable and time-dependent, nor are they sent out over the communication network - as is the SecureCode of the present invention.

Another fundamental difference with respect to Brachtl is that determination of a valid PIN takes place at the EFT terminal (abstract, col. 5 lines 3-8). Conversely, the SecureCode of the present invention allows User verification to take place at the Central-Entity – hence avoiding any need for EFT terminals or personal identity cards.

For the above described reasons, Applicants' respectfully submit that claim 5 is also allowable over the prior art.

**Conclusion**

Accordingly, Applicants' respectfully request reconsideration of the claim rejections based on the above amendments and remarks. It is believed that a full and complete response has been made to the outstanding Office Action, and as such, the present application is in condition for allowance. If the examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (571) 228-2938.

Dated: 11/28/2005

Respectfully submitted,

By: 

Shawna J. Shaw  
Agent for Applicants  
Registration No. 57,091